RED REVISTA ESTRATEGIA E DESENVOLVIMENTO

ISSN – 2526-9526

Efetividade dos Controles em um Sistema de Contabilidade para Instituições Financeiras: percepções dos analistas, desenvolvedores e usuários

Effectiveness of Controls in an Accounting System for Financial Institutions: perceptions of analysts, developers and users

Efectividad de los Controles en un Sistema de Contabilidad para Instituciones Financieras: percepciones de los analistas, desarrolladores y usuarios

Recebido em: 20 de Dezembro de 2018
Aprovado em: 07 de Junho de 2019
Avaliado pelo sistema double blind review
Editoria Científica: Carolina Freddo Fleck

Stéfani Piccin (stefanipiccin@gmail.com)- UFRGS
Ariel Behr
Fernanda da Silva Momo

RESUMO

A segurança da informação tornou-se fundamental para proteção das informações nas instituições. Nesse sentido, o objetivo desta pesquisa é apresentar as percepções dos analistas, desenvolvedores e usuários sobre a efetividade dos controles de acesso presentes em um Sistema de Contabilidade para Instituições Financeiras, através da realização de entrevistas com pessoas chaves destes grupos e da análise da documentação do sistema. Quanto aos procedimentos metodológicos, a pesquisa é classificada como qualitativa, descritiva e estudo de caso. A amostra compreendeu analistas e desenvolvedores de uma grande empresa multinacional desenvolvedora de software de gestão empresarial e usuários do sistema de três Instituições Financeiras de relevância no mercado. Os resultados evidenciam que nas percepções dos analistas, desenvolvedores e usuários os controles presentes no Sistema de Contabilidade são efetivos, uma vez que limitam o acesso às funcionalidades e relatórios do sistema somente aos usuários autorizados. Quanto a importância da segurança da informação, verificou-se que embora as instituições adotem políticas de segurança e estão preocupadas em proteger suas informações, nas percepções dos analistas e desenvolvedores a maioria dos usuários reconhece a relevância dos controles de acesso somente quando ocorre algum tipo de incidente envolvendo segurança da informação. Os resultados apontam que é imprescindível que os usuários de sistemas de informação compreendam o valor da segurança da informação para que pratiquem um comportamento adequado na realização das suas atividades. Além disso, verificou-se que as percepções dos usuários podem auxiliar na formulação de políticas de segurança mais efetivas nas organizações.

ISSN – 2526-9526

Palavras-chave: Segurança da Informação. Sistema de Contabilidade. Controles de Acesso.

ABSTRACT

Information security has become essential for the protection of information in institutions. In this sense, the objective of this research is to present the perceptions of analysts, developers and users about the effectiveness of the access controls present in an Accounting System for Financial Institutions, through interviews with key people of these groups and the analysis of the documentation of the system. As for the methodological procedures, the research is classified as qualitative, descriptive and case study. The sample included analysts and developers of a large multinational company that develops business management software and system users of three Financial Institutions of relevance in the market. The results show that in the perceptions of analysts, developers and users the controls present in the Accounting System are effective, since they limit access to the system's functionalities and reports only to authorized users. Regarding the importance of information security, it was found that although institutions adopt security policies and are concerned with protecting their information, in the perceptions of analysts and developers, most users recognize the relevance of access controls only when some type of incident involving information security. The results point out that it is imperative that users of information systems understand the value of information security to practice appropriate behavior in carrying out their activities. In addition, it was verified that user perceptions can help in the formulation of more effective security policies in organizations.

Keywords: Information Security. Accounting system. Access Controls.

RESUMEN

La seguridad de la información se ha vuelto fundamental para proteger la información en las instituciones. En este sentido, el objetivo de esta investigación es presentar las percepciones de los analistas, desarrolladores y usuarios sobre la efectividad de los controles de acceso presentes en un Sistema de Contabilidad para Instituciones Financieras, a través de la realización de entrevistas con personas claves de estos grupos y del análisis de la documentación del documento sistema. En cuanto a los procedimientos metodológicos, la investigación es clasificada como cualitativa, descriptiva y estudio de caso. La muestra comprendió analistas y desarrolladores de una gran empresa multinacional desarrolladora de software de gestión empresarial y usuarios del sistema de tres Instituciones Financieras de relevancia en el mercado. Los resultados evidencian que en las percepciones de los analistas, desarrolladores y usuarios los controles presentes en el sistema de contabilidad son efectivos, ya que limitan el acceso a las funcionalidades e informes del sistema sólo a los usuarios autorizados. En cuanto a la importancia de la seguridad de la información, se verificó que aunque las instituciones adopta políticas de seguridad y están preocupadas por proteger su información, en las percepciones de los analistas y los desarrolladores, la

ISSN – 2526-9526

mayoría de los usuarios reconoce la relevancia de los controles de acceso sólo cuando ocurre algún tipo de incidentes relacionados con la seguridad de la información. Los resultados apuntan que es imprescindible que los usuarios de sistemas de información comprendan el valor de la seguridad de la información para que practiquen un comportamiento adecuado en la realización de sus actividades. Además, se verificó que las percepciones de los usuarios pueden auxiliar en la formulación de políticas de seguridad más efectivas en las organizaciones.

Palabras-claves: Seguridad de la Información. Sistema de Contabilidad. Controles de acceso.

1 INTRODUÇÃO

Trabalhar de forma mais ágil e competitiva tornou-se uma necessidade para as organizações. Compreender e aprimorar o gerenciamento dos processos do negócio passou a ser essencial para garantir a continuidade operacional de uma instituição no mercado. Entre os fatores que podem contribuir para que uma organização se mantenha viva e apresente vantagens competitivas em relação aos seus concorrentes, pode-se citar os sistemas de informação utilizados por ela.

Autores como Rainer Jr e Cegielski (2011) destacam que os sistemas de Tecnologia da Informação (TI) são parte integrante de todos os departamentos funcionais de uma empresa. Salientam também, que nos setores de finanças e contabilidade, os gerentes usam sistemas para estimar os lucros nas atividades comerciais, determinar as melhores fontes e uso dos recursos e realizar auditorias a fim de assegurar que a organização é sólida e que os relatórios e documentos emitidos são corretos e confiáveis.

A TI desempenha um papel importante em vários setores de uma organização, pois fornece informações úteis para tomada de decisão e definição de estratégias. Em virtude da significância das informações geradas nos sistemas de informação, as instituições estão cada vez mais preocupadas com a segurança e privacidade da informação, visto que o mau uso das tecnologias pode proporcionar o vazamento de informações confidenciais.

Baltzan e Phillips (2012) descrevem que segurança da informação se trata de um termo amplo, que contempla a proteção da informação contra mau uso acidental ou intencional por pessoas dentro ou fora da empresa. Os autores sugerem, também, que todas as empresas precisam entender o valor da segurança da informação, mesmo que não seja obrigatório por lei. No caso das Instituições Financeiras, com o grande volume de operações realizadas diariamente, evidencia-se a importância e a essencialidade dos controles presentes nos sistemas de informação para garantir maior segurança e confidencialidade das informações.

Assim, a questão problema que motiva esta pesquisa é: Quais as percepções dos analistas, desenvolvedores e usuários sobre a efetividade dos controles presentes em um Sistema de Contabilidade para Instituições Financeiras tendo em vista os atributos da segurança da informação? Diante disso, o objetivo geral deste estudo é apresentar as percepções desses atores sobre a efetividade dos controles presentes em um Sistema de Contabilidade para Instituições Financeiras.

ISSN – 2526-9526

Os sistemas contábeis geram informações valiosas sobre uma organização. Nas Instituições Financeiras, além da escrituração contábil, os sistemas são utilizados para geração de documentos exigidos pelo Banco Central do Brasil (BACEN) e como base para geração de outras informações enviadas à Receita Federal do Brasil (RFB). As informações remetidas ao BACEN e à RFB, devem ser íntegras e representar a realidade da Instituição Financeira, fato que reforça o valor da segurança da informação em um Sistema de Contabilidade e a escolha por esta temática.

Ademais, a segurança da informação é um assunto atual e relevante, uma vez que trata de questões que impactam tanto o ambiente pessoal como o corporativo. Quanto a importância acadêmica, espera-se contribuir com informações oportunas relacionadas à segurança da informação no âmbito da pesquisa contábil e que estas informações possam colaborar para mitigar os problemas envolvendo segurança da informação nas instituições.

Em relação aos limites da pesquisa, o estudo delimitou-se a analisar as percepções dos analistas, desenvolvedores e usuários sobre efetividade dos controles de acesso presentes em um Sistema de Contabilidade para Instituições Financeiras. Para isso, realizou-se um estudo de caso em uma empresa do setor de TI onde os dados foram coletados por meio de entrevistas e a partir da análise de documentos do sistema.

Esta pesquisa está estruturada em cinco seções, incluindo esta introdução. Na segunda seção, explana-se o referencial teórico que embasa o estudo. Na terceira, descrevem-se os procedimentos metodológicos, enquanto que na quarta, são apresentados e analisados os principais resultados obtidos. Na quinta seção, constam as considerações finais do estudo.

2 SEGURANÇA DA INFORMAÇÃO

Atualmente, a segurança da informação é uma das preocupações que mais atingem as corporações, uma vez que os sistemas de informação estão expostos a diversos riscos e ameaças, tais como fraude, erro, interrupção e atraso de serviços, revelação de informações confidenciais, roubo e manipulação de informações (HURT, 2014). Diante deste cenário de riscos e ameaças, Baltzan e Phillips (2012) sugerem que as empresas devem registrar políticas de segurança da informação e estabelecer procedimentos para orientar os funcionários a fim de proteger a instituição da má utilização dos sistemas de informação e recursos de TI.

De acordo com Fontes (2010), os regulamentos de segurança da informação objetivam que o uso da informação na instituição ocorra de maneira estruturada e que o negócio não seja prejudicado por mau uso da informação, seja por erro ou de forma intencional. Hurt (2014) ressalta que informar as funções e responsabilidades dos funcionários de acordo com as políticas de segurança deve ser a primeira linha de defesa para proteção das infraestruturas computacionais de uma instituição. Na concepção de Imoniana (2011), qualquer instituição que opere com TI necessita de segurança de forma proporcional ao grau de complexidade do seu ambiente operacional.

Imoniana (2011, p.46) salienta que "a segurança em sistema computadorizado é muito importante não somente em termos de proteção física dos dados, mas, também para prevenir ocorrências de incidentes fatais, que podem causar estragos irreparáveis em documentos e programas vitais". A autora destaca ainda que com o aumento da

ISSN – 2526-9526

necessidade de segurança verificada atualmente, os usuários de sistemas estão mais conscientizados e aceitam os controles de acesso com maior naturalidade.

Para facilitar a implementação de controles de segurança, a série de normas ISO/IEC 27000, publicadas pela Associação Brasileira de Normas Técnicas (ABNT) no Brasil, determinam elementos primordiais na elaboração de políticas de segurança da informação nas organizações. Neste conjunto de normas, destacam-se a ISO/IEC 27001 que aborda os requisitos para os sistemas de gestão da segurança da informação (ABNT, 2013) e a ISO/IEC 27002 que trata das práticas de sistemas de gestão da segurança da informação e estabelece diretrizes gerais para implementar, manter e melhorar a gestão de segurança da informação em uma organização (ABNT, 2013).

A segurança da informação é definida na norma ISO/IEC 27002, como a proteção da informação contra vários tipos de ameaças, a fim de garantir a continuidade, minimizar os riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócios (ABNT, 2013). Nesta perspectiva, para implementação de práticas de segurança da informação as instituições devem seguir como norte os atributos básicos apresentados na norma ISO/IEC 27002 (ABNT, 2013): a) Confidencialidade: limita o acesso à informação para elementos não autorizados (pessoas, organizações, processos); b) Integridade: assegura a exatidão da informação conforme suas características originais; c) Disponibilidade: garante que a informação esteja acessível sempre que necessária para elementos autorizados; d) Autenticidade: garante que a informação é proveniente do remetente relacionado e não sofreu alterações durante o envio; e) Irretratabilidade (não-repúdio): impossibilidade de negar autoria de uma transação realizada.

Além destes princípios, a norma de segurança ISO/IEC 27002 recomenda que sejam implementados controles para garantir a redução de riscos (ABNT, 2013). Estes controles podem ser classificados como controles físicos ou controles lógicos de acessos. Os controles físicos são necessários basicamente para proteção de computadores e equipamentos, a fim de evitar roubos, destruição ou danos causados por acidentes e impedir que indivíduos não autorizados acessem o local onde se encontram estes equipamentos (HURT, 2014).

Por outro lado, os controles lógicos referem-se aos recursos tecnológicos de um sistema contra acessos não autorizados aos dados ou informações não permitidas para usuários específicos. Estes controles envolvem a utilização de garantias incorporadas em hardware e softwares, como senhas, criptografia, software de controle de acesso, entre outros recursos (RAINER JR; CEGIELSKI, 2011). Rainer Jr e Cegielski (2011) destacam também, que os controles lógicos de acesso contemplam duas funções principais: autenticação e autorização de usuários. A autenticação determina a identidade do usuário que está tentando o acesso e a autorização determina as ações ou privilégios o usuário possui a partir da identidade verificada.

Neste sentido, Hurt (2014) explana que os controles de acesso geralmente podem ser vistos como um processo de três etapas: identificação (o usuário fornece informações para que o sistema o reconheça), autenticação (uma vez identificado, o usuário deve provar a sua identidade) e autorização (o usuário recebe as prerrogativas associadas a seu perfil). Quanto ao processo de autorização, Beal (2007) salienta que a utilização de perfis para grupo de usuários com necessidades diferentes, possibilita gerenciar de forma mais eficiente os privilégios de acesso de um sistema, facilitando o processo de

ISSN – 2526-9526

mudança quando necessário ampliar ou reduzir as permissões de acesso de determinado grupo de usuários.

A autora destaca ainda que é importante garantir que os privilégios concedidos sejam adequados às reais necessidades dos usuários, de forma que não contemplem autorizações desnecessárias para execução do trabalho ou que possam colocar em risco a segurança das informações da instituição (BEAL, 2007). Acerca da administração dos privilégios de acesso concedidos aos usuários, Imoniana (2011) destaca que nos sistemas de informações contábeis é comum a utilização de testes de compatibilidade de funções antes da liberação de acessos, para que o usuário acesse somente os dados e funcionalidades do sistema que ele realmente pode e necessita acessar.

Tendo em vista a relevância das informações geradas nos sistemas contábeis, pode-se afirmar que os controles de acesso são fundamentais para promover maior segurança da informação, pois conforme explana Hurt (2014) a incapacidade de proteger as informações de uma organização pode levar a perdas financeiras, ações judiciais e perda de confiança no mercado.

2.1 SEGURANÇA DA INFORMAÇÃO CONTÁBIL

A contabilidade é uma ciência social que busca examinar, interpretar e registrar os fenômenos que afetam o patrimônio de uma entidade (ARAÚJO; ASSAF NETO, 2010). Esta ciência apresenta como principal objetivo "captar todos os fatos que estão ocorrendo na empresa, registrar tais fatos num sistema de informação, acumular os fatos nesse sistema, resumir os acontecimentos num certo período de tempo, criar e emitir um resumo que servirá de suporte para interpretar todo o processo e resultados" (ARAÚJO; ASSAF NETO, 2010, p.4).

Embasado neste objetivo, constata-se que a contabilidade tem a missão de fornecer informações úteis e confiáveis aos usuários, com o propósito de suprir suas necessidades e subsidiá-los nas decisões. No entanto, cabe ressaltar, que estas informações devem ser de fácil compreensão, pois só assim viabilizarão a geração de benefícios econômicos à instituição. Nesse sentido, ressalta-se o papel da contabilidade e por consequência dos sistemas de informações contábeis utilizados pelas corporações, visto que "o sistema de informação contábil processa dados e os transforma em informações contábeis úteis para o processo decisório de toda a empresa, para todos os níveis" (PADOVEZE, 2009, p.128).

Hurt (2014) expõe que um sistema de informação contábil pode ser definido como um conjunto de atividades inter-relacionadas, documentos e tecnologias destinados a coletar dados, processá-los e relatar informações para um grupo de tomadores de decisões internos e externos nas organizações. No processo de transformação dos dados em informações contábeis úteis, Padoveze (2009) descreve que são necessários pelo menos dois recursos: contadores com capacitação adequada para o enfoque sistêmico da contabilidade e um software de contabilidade que viabilize ao contador efetivar todo o potencial gerencial da informação a ser gerada e utilizada. Considerando esses aspectos, evidencia-se a importância da utilização de um sistema de informação contábil que responda adequadamente às necessidades de informações dos usuários e que apresente níveis de segurança, capacidade de rastreabilidade dos dados e

ISSN – 2526-9526

informações, controle e alerta sobre acessos indevidos, entre outras funcionalidades que garantam maior segurança das informações (PADOVEZE, 2009).

Para Hurt (2014) os controles internos tem sido o cerne dos sistemas de informações contábeis, uma vez que apresentam quatro propósitos principais: proteger ativos, garantir demonstrações contábeis confiáveis, incentivar o cumprimento de regras de gestão e promover a eficiência operacional. O autor salienta também, que atualmente com a transformação da internet em ferramenta para troca de informações globais, os sistemas de informações contábeis e as informações que eles armazenam e processam cada vez mais serão vítimas de crimes e fraudes virtuais (HURT, 2014), fato que reforça a importância da segurança da informação para proteção das informações das instituições.

Tendo em vista essas reflexões, Silva (2013) realizou um estudo sobre a percepção dos usuários da informação contábil a respeito da segurança da informação nas organizações com base em seis elementos da segurança da informação (Integridade, Disponibilidade, Confidencialidade, Equipamentos, Políticas e Procedimentos e Pessoas). A análise foi direcionada para a contabilidade, tendo em vista que é a área responsável por consolidar todas as informações de uma instituição. Os resultados encontrados evidenciaram que os usuários da informação contábil estão conscientes da importância da segurança da informação. No entanto, verificou-se insatisfação em relação aos recursos, políticas e procedimentos utilizados para garantir a segurança da informação nas organizações onde trabalham. Os resultados indicam também que as empresas não estão utilizando ou divulgando de forma adequada estes procedimentos. Além disso, constatou-se indícios de que as organizações enfrentam dificuldades para controlar o componente humano da segurança da informação.

Klein (2014) buscou através de uma análise comportamental do usuário, compreender até que ponto a percepção humana sobre ameaça, esforço, controle e descontentamento podem induzir a um comportamento responsável quanto à segurança da informação e como esse comportamento pode gerar vulnerabilidade e possíveis violações na segurança da informação. Os dados obtidos indicaram que as orientações sobre segurança da informação influenciam na percepção do usuário em relação a identificação da severidade das ameaças. Examinou-se ainda, a importância de capacitações periódicas para possibilitar que os usuários compreendam a necessidade de segurança, a gravidade dos danos que podem ser causados, os benefícios gerados pelos controles, bem como a sua responsabilidade diante das informações da organização onde atuam. O estudo enfatiza que a partir desta conscientização, os usuários serão motivados a praticar um comportamento adequado quanto à segurança da informação.

3 PROCEDIMENTOS METODOLÓGICOS

Quanto à forma de abordagem do problema, classifica-se como qualitativa, pois visa apresentar e aprofundar o entendimento das percepções dos analistas, desenvolvedores e usuários sobre a efetividade dos controles presentes no Sistema de Contabilidade que utilizam. A respeito deste tipo de abordagem, autores como Gerhardt e Silveira (2009) salientam que a pesquisa qualitativa está voltada para o

ISSN – 2526-9526

aprofundamento da compreensão de uma organização, e não para a representatividade numérica, definição que reforça a escolha por esta abordagem.

No que se refere aos objetivos, trata-se de uma pesquisa descritiva, na medida em que se propõe a descrever as principais características dos controles de acesso do sistema e as percepções dos atores deste estudo em relação a sua efetividade. Gil (1999), explica que o principal objetivo deste tipo de pesquisa é descrever características de uma determinada população ou fenômeno ou determinar relações entre as variáveis. Em relação aos procedimentos técnicos, a pesquisa qualifica-se como estudo de caso, pois conforme explana Yin (2005, p.32) um estudo de caso "investiga um fenômeno contemporâneo dentro do seu contexto da vida real, especialmente quando o fenômeno e o contexto não estão claramente definidos".

A população alvo deste estudo foi definida como profissionais da área de TI e usuários de sistemas de informações contábeis atuantes no segmento financeiro no estado do Rio Grande do Sul. Em relação a amostra, optou-se por uma amostragem do tipo não probabilística por julgamento, uma vez que para viabilizar a análise das percepções, foram selecionados três grupos (analistas, desenvolvedores e usuários) com visões distintas sobre os controles de acesso presentes no Sistema de Contabilidade. É oportuno salientar, que os analistas e desenvolvedores são participantes de uma grande empresa multinacional que é uma das maiores provedoras de software de gestão empresarial (ERP) no mercado nacional e internacional e os usuários são membros de Instituições Financeiras de relevância no mercado brasileiro.

Como técnica para coleta de dados, foram realizadas entrevistas do tipo estruturadas com pessoas chaves destes três grupos entre os meses de janeiro e fevereiro de 2018. Além disso, foram coletadas informações do sistema através da análise de manuais e relatórios. No quadro 1 verifica-se a caracterização dos entrevistados:

Quadro 1 - Perfil dos Entrevistados

Entrevistado	Categoria	Idade	Sexo	Tempo atuação na área
Entrevistado 1	Analista de Negócios	35 anos	Feminino	5 anos
Entrevistado 2	Analista de Negócios	25 anos	Feminino	2 anos
Entrevistado 3	Analista de Negócios	39 anos	Feminino	6 anos
Entrevistado 4	Desenvolvedora	39 anos	Feminino	17 anos
Entrevistado 5	Desenvolvedor	35 anos	Masculino	10 anos
Entrevistado 6	Desenvolvedor	38 anos	Masculino	15 anos
Entrevistado 7	Desenvolvedor	35 anos	Masculino	10 anos
Entrevistado 8	Usuário	25 anos	Masculino	5 anos
Entrevistado 9	Usuário	30 anos	Masculino	7 anos
Entrevistado 10	Usuário	36 anos	Feminino	6 anos

Fonte: elaborado a partir dos dados da pesquisa (2018).

Quanto à análise e interpretação dos dados, optou-se pela análise de conteúdo, a qual contemplou etapas de pré-análise, categorização dos dados e descrição e interpretação dos dados para verificar as percepções dos atores deste estudo em relação a efetividade dos controles de acesso presentes no Sistema de Contabilidade. Destaca-se, portanto, a não possibilidade de generalização dos resultados deste estudo.

ISSN – 2526-9526

4 ANÁLISE DOS DADOS

4.1 CONTROLES DE ACESSO PRESENTES NO SISTEMA DE CONTABILIDADE

Para identificação e entendimento dos controles de acesso presentes no Sistema de Contabilidade foi utilizado o manual do sistema e explorado o processo de liberação de acessos. A partir da análise realizada, verificou-se que o cadastro de usuários e as permissões de acesso às funcionalidades e relatórios do Sistema de Contabilidade são realizados por outro *software,* chamado Sistema de Segurança.

Com isso, a seguir serão abordadas as principais funcionalidades do Sistema de Segurança utilizadas para realizar os controles de acesso ao Sistema de Contabilidade: Perfis de Acesso, Cadastro de Usuários, Configurações e Auditoria.

4.1.1 PERFIS DE ACESSO

O cadastro de perfis de acesso permite a definição de um conjunto de autorizações de acesso comum a um ou mais usuários e representam as atividades que cada grupo de usuários poderá executar no sistema. A criação e manutenção dos perfis é realizada pelo administrador da instituição e contempla três etapas: criação, autorização e associação de perfis e relatórios.

Inicialmente, o administrador define uma sigla e descrição para identificação do perfil, o seu nível operacional e indica se é privilegiado ou não. Ao assinalar a opção privilegiado, o perfil terá acesso a todas as funcionalidades do sistema, ou seja, mesmo que seja configurada uma restrição de acesso para este perfil, ela não terá validade sobre ele. A figura 1 apresenta a tela de cadastro de Perfis de Acesso.

Figura 1 - Cadastro de Perfil de Acesso

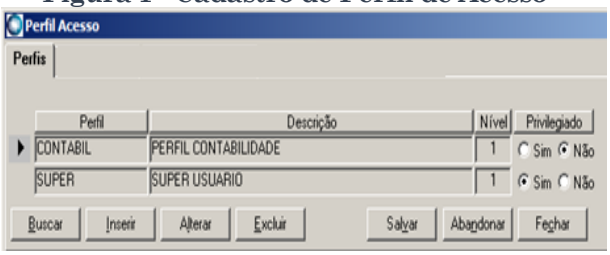


Figura 2 - Autorizações de Acesso

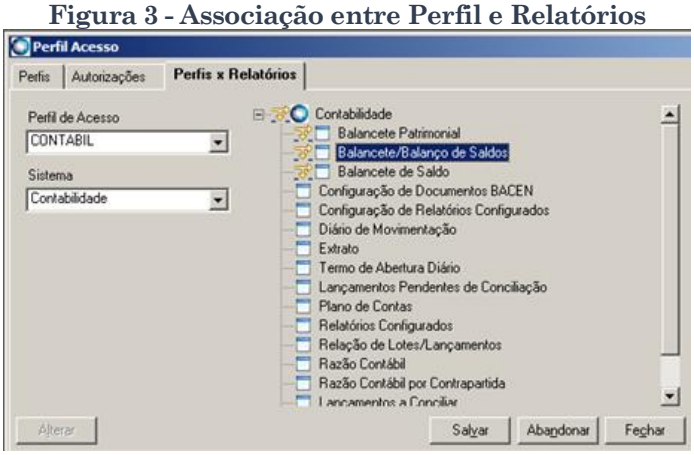
Fonte: Sistema de Segurança (2018).

Após o cadastro, o administrador define as transações do Sistema de Contabilidade que o perfil terá permissão de acesso, sendo possível conceder acesso ao sistema inteiro, menus, telas ou somente funções específicas (botões). A figura 2 apresenta a tela onde são realizadas as autorizações de acesso.

O ícone "setinhas amarelas" ao lado das transações, indica que o perfil selecionado possui autorização para acessar as transações do Sistema de Contabilidade. Além das autorizações às funcionalidades, o administrador determina os relatórios do Sistema de Contabilidade que poderão ser gerados pelo perfil, conforme ilustra a figura 3:

ISSN – 2526-9526

Figura 3 - Associação entre Perfil e Relatórios



Fonte: Sistema de Segurança (2018).

A partir destas configurações, verificou-se que através da criação de perfis de acesso é possível conceder acesso somente as funcionalidades e relatórios que os usuários realmente podem e necessitam acessar no Sistema de Contabilidade, o que contribui para a segurança da informação da instituição.

4.1.2 CADASTRO DE USUÁRIOS

O cadastro de usuários também é responsabilidade do administrador da instituição e envolve duas etapas: cadastro e definição de restrições de acesso. No cadastramento, realiza-se a manutenção das características individuais do usuário, define-se a sua amplitude de acesso, verifica-se as informações de acesso, os acessos a sistemas de gestão e as informações para renovação da senha, como pode ser verificado na figura 4:

Figura 4 - Cadastro de Usuários

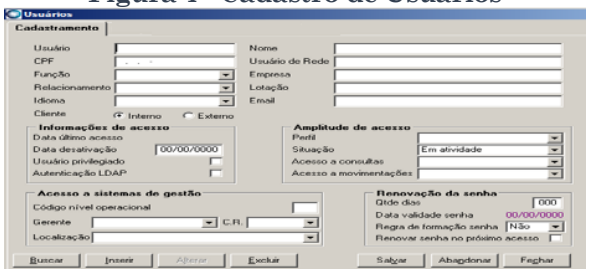
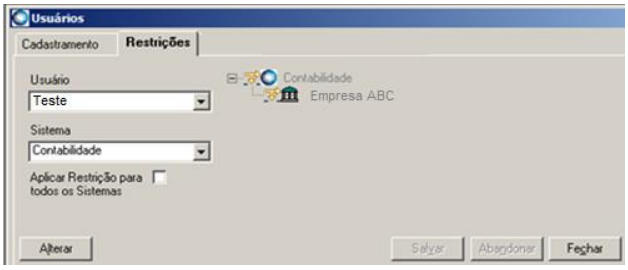


Figura 5 - Restrições de acesso: empresas e unidades



Fonte: Sistema de Segurança (2018).

Após realizar o cadastro, na aba Restrições são definidas as empresas e unidades que o usuário terá permissão de acesso no Sistema de Contabilidade, conforme pode ser verificado na figura 5. Esta configuração é fundamental para garantir que o usuário acessará somente a amplitude organizacional pertinente as suas atividades no Sistema de Contabilidade.

ISSN – 2526-9526

4.1.3 CONFIGURAÇÕES

O Sistema de Segurança possui um menu de Configurações onde são definidas as regras para controle de validade de senha para ou usuários internos ou externos da instituição. A figura 6 apresenta a tela destinada as configurações destas regras:

Figura 6 - Cadastro de regras de validade de senhas

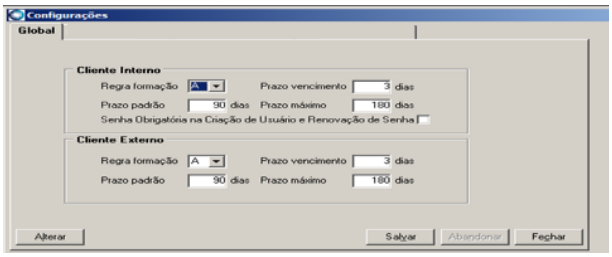
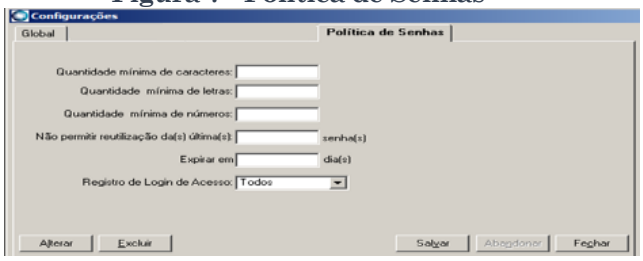


Figura 7 - Política de Senhas



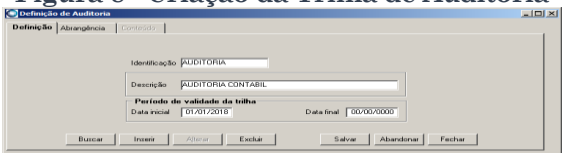
Fonte: Sistema de Segurança (2018).

Ainda neste menu, o sistema possibilita a configuração de uma política de senhas para criação de regras que servirão de base ao cadastrar ou renovar a senha dos usuários. A figura 7 apresenta a tela de cadastro de Política de Senhas. Essas regras e políticas de senhas são assumidas no cadastramento da senha do usuário e contribuem para o controle e segurança das senhas utilizadas pelos usuários dos sistemas.

4.1.4 AUDITORIA

O Sistema de Segurança possui uma funcionalidade de auditoria, a qual permite que o administrador configure trilhas de auditoria para registrar os acessos e alterações efetuadas nos demais sistemas controlados pelo Sistema de Segurança. A figura 8 apresenta a tela para criação da trilha de auditoria:

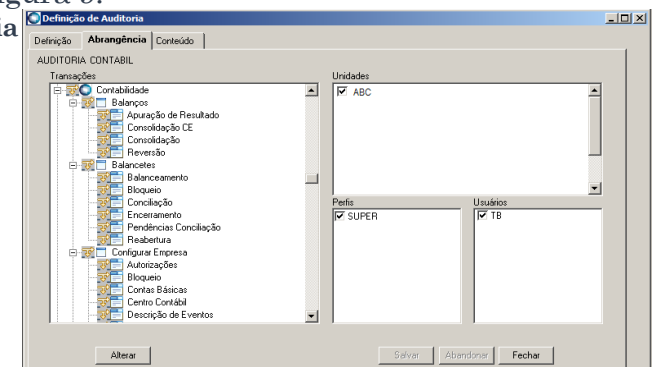
Figura 8 - Criação da Trilha de Auditoria



Fonte: Sistema de Segurança (2018).

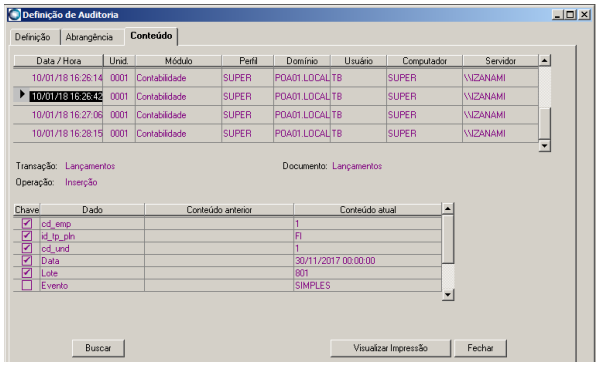
Após a criação, o administrador determina a abrangência da trilha de auditoria, ou seja, as transações do sistema, as empresas/unidades, os perfis e os usuários que serão auditados, conforme verifica-se na figura 9:

Figura 9 - Abrangência da Trilha de Auditoria



ISSN – 2526-9526

Figura 10 - Registros da Trilha de Auditoria



Fonte: Sistema de Segurança (2018).

Importante destacar, que a trilha de auditoria só registra as alterações a partir da data inicial informada na tela de criação. Na aba Conteúdo, o sistema apresenta as informações gravadas pela trilha de auditoria, tais como data e hora do acesso, unidade onde foi realizado o acesso, módulo, perfil, usuário, a operação (inserção, atualização, exclusão), transação, os campos alterados, conteúdo anterior e o conteúdo atual, como pode ser visto na figura 10:

Além da visualização em tela, o sistema possibilita que o usuário faça a impressão do relatório contendo todas estas informações. Esta é uma funcionalidade que permite a rastreabilidade das ações realizadas pelos usuários do sistema e a sua utilização pode contribuir para a segurança da informação.

4.2 CONTROLES IMPLEMENTADOS NAS FUNCIONALIDADES DO SISTEMA DE CONTABILIDADE

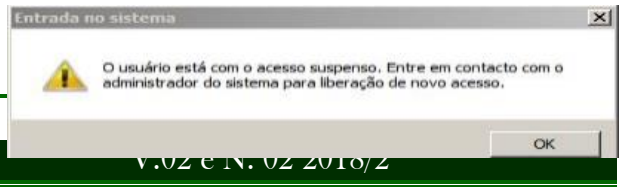
O Sistema de Contabilidade estudado pode ser utilizado por qualquer tipo de empresa. No entanto, apresenta como diferencial atender às necessidades contábeis e legais específicas das Instituições Financeiras, sobretudo as normas e exigências do BACEN. Diante da relevância das informações enviadas ao BACEN, é fundamental que as informações geradas no Sistema de Contabilidade sejam íntegras e confiáveis.

A partir desta perspectiva, analisou-se como ocorre o acesso ao Sistema de Contabilidade e as principais regras presentes nas seguintes funcionalidades do sistema: Plano de Contas, Integração de lançamentos via *Interfaces* e lançamentos manuais, Fechamento e reabertura de período, Apuração de resultados, Documentos BACEN e Geração e configurações de relatórios.

4.2.1 AUTENTICAÇÃO DO USUÁRIO E ABRANGÊNCIA DE ACESSO

Com base na análise realizada, constatou-se que o primeiro passo para que o usuário acesse o Sistema de Contabilidade é a autenticação do usuário através da informação do usuário e senha cadastrado no Sistema de Segurança, conforme pode ser verificado na figura 11:

Figura 11 -Autenticação do Usuário



ISSN – 2526-9526

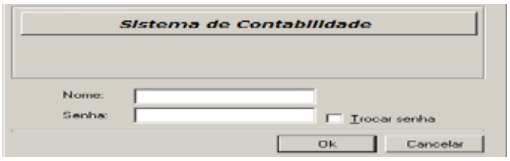


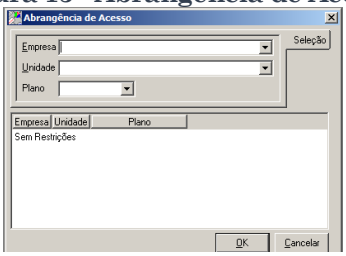
Figura 12 – Mensagem de usuário suspenso

Fonte: Adaptado de Sistema de Contabilidade (2018).

Caso o usuário erre os dados de acesso, após atingir o número de tentativas parametrizadas no Sistema de Segurança, o sistema bloqueia o usuário como pode ser verificado na figura 12.

Após a autenticação, o usuário seleciona a abrangência de acesso (empresa, unidade e plano) que deseja acessar no Sistema de Contabilidade, conforme mostra a figura 13.

Figura 13 - Abrangência de Acesso



Fonte: Sistema de Contabilidade (2018).

Constatou-se que o usuário consegue acessar somente a empresa e unidade que lhe foi concedido acesso no Sistema de Segurança. Os resultados da pesquisa indicam que esta restrição é essencial, pois na maioria das instituições existe mais de uma empresa e/ou unidades.

Verificou-se também, que após acessar o sistema, o usuário visualiza apenas os menus, telas, transações e relatórios que foram autorizados para o seu perfil de acesso no Sistema de Segurança. Estas restrições de acesso são essenciais, uma vez que evitam que usuários sem autorização acessem, visualizem informações, gerem relatórios ou realizem operações em empresas ou unidades que não deveriam ter acesso.

4.2.2 PLANO DE CONTAS

Por definição do BACEN, as Instituições Financeiras são obrigadas a adotar a estrutura hierárquica do Plano de Contas COSIF (Plano Contábil das Instituições do Sistema Financeiro Nacional) até o 5º (quinto) nível (contas sintéticas), podendo cadastrar as suas contas analíticas (contas que recebem lançamentos) a partir do 6º (sexto) nível.

A utilização de um Plano de Contas padronizado objetiva uniformizar os registros contábeis, facilitar o monitoramento financeiro das instituições e fomentar o controle do risco sistêmico.

Para assegurar que as contas serão cadastradas de acordo com a estrutura COSIF, o sistema possui uma regra que habilita a tela de cadastro do Plano de Contas somente após a configuração da estrutura dos níveis das contas contábeis. Esta configuração é fundamental, tendo em vista que os Documentos remetidos ao BACEN

ISSN – 2526-9526

devem ser gerados e apresentar os códigos das contas contábeis de acordo com o COSIF até o 5º (quinto) nível.

Identificou-se também, que após a informação do código da conta, o sistema classifica automaticamente a classe (ativo ou passivo), tipo (analítica ou totalizadora), natureza (credora ou devedora), entre outros atributos da conta. Esta classificação automática é um fator importante, uma vez que diminui a possibilidade de cadastro incorreto da conta.

Além disso, o sistema permite restringir a utilização de uma conta contábil por perfil de acesso, impossibilitando assim, que usuários de perfis não autorizados façam lançamentos em uma conta contábil que não deveriam ter acesso. Possibilita também, que seja configurado um período de dias máximo para aceitação de lançamentos retroativos na conta, de maneira que, se um usuário tentar realizar lançamentos para um período maior, o sistema não permite a inclusão do lançamento.

Constatou-se ainda que o sistema possui regras que impedem a exclusão de contas que já receberam movimentação contábil, permitindo apenas que o usuário desative a conta. Nesta perspectiva, as regras e controles implementados no cadastro de contas contribuem para a confidencialidade e integridade das informações geradas no Sistema de Contabilidade.

4.2.3 INTEGRAÇÃO DE LANÇAMENTOS VIA *INTERFACES* E LANÇAMENTOS MANUAIS

No Sistema de Contabilidade, a contabilização dos lançamentos pode ser realizada via integração de *interfaces* (arquivos ou banco de dados) ou através de lançamentos manuais.

Para viabilizar a integração de lançamentos via *interface*, é necessário que o administrador realize o cadastro e configurações das *interfaces*, tais como, sigla de identificação, faixa de numeração de lotes, periodicidade, *layout* utilizado, entre outros critérios a serem adotados pelo sistema no momento do processamento da *interface.*

O sistema conta também com a opção de integração via banco de dados. Esta opção permite que sistemas legados possam gerar as informações diretamente nas tabelas do banco de dados em vez de gerá-las em arquivos de contabilização, característica que contribui para a segurança da informação, pois impede que os arquivos sejam manipulados.

Na rotina de integração de *interfaces*, o sistema possui diversas regras que validam os lançamentos antes de concluir a integração. O sistema verifica, por exemplo, se o total de débitos e créditos fecham, se todas as contas informadas no arquivo estão cadastradas no Plano de Contas, se a data do lançamento é um dia útil, entre outras validações.

Caso o sistema identifique alguma divergência, o arquivo é rejeitado e os lançamentos não são integrados no Sistema de Contabilidade. Neste caso, o usuário precisa corrigir a inconsistência no sistema de origem, gerar o arquivo novamente e na sequência integrá-lo no sistema.

Na tela de integração de *interfaces*, o sistema registra o *status* da integração, a data e horário, o usuário e a quantidade de lançamentos integrados. O sistema também possui um relatório onde é possível verificar os lotes integrados, a origem dos

ISSN – 2526-9526

lançamentos, o usuário que realizou a integração e se houve alteração no lote após a integração, entre outras informações.

Além da integração de lançamentos via *interface*, o Sistema de Contabilidade permite a inclusão, alteração ou exclusão de lançamentos contábeis por processo manual. Na inclusão de lançamentos manuais o sistema também realiza validações de valores, datas, contas, histórico, etc. Os lançamentos manuais podem ser visualizados no relatório de lotes, da mesma forma que os lançamentos integrados via *interface.*

Tanto para as integrações via *interface* quanto para os lançamentos manuais, o sistema possui uma configuração opcional de "Perfil 2ª Assinatura". Se esta opção for configurada, o lançamento contábil incluído por um usuário operador, por exemplo, somente sensibilizará o saldo de uma conta contábil se o usuário com perfil autorizador assinar (autorizar) o lote.

Além disso, o sistema permite configurar dados gerenciais para os lançamentos tais como, centro de custo do lançamento, gerente responsável, a área do responsável do lançamento e o código do cliente do lançamento. Examinou-se que todas estas regras implementas na rotina de lançamentos contribuem para que as informações geradas no Sistema de Contabilidade sejam íntegras, disponíveis e confiáveis.

4.2.4 FECHAMENTO E REABERTURA DE PERÍODO

A funcionalidade de fechamento é utilizada para realizar o encerramento do dia/mês no Sistema de Contabilidade. A execução deste processamento pode ser diária ou mensal e deve ser avaliada pelo responsável da área, pois após a execução, o sistema não permite que sejam realizados lançamentos contábeis para uma data já encerrada.

A opção de reabertura é utilizada somente para os casos em que por algum motivo específico, o usuário precisa incluir um lançamento para uma data já encerrada. Devido à importância destas funcionalidades e do impacto que podem causar para a contabilidade da instituição, examinou-se que as instituições concedem acesso somente para os gerentes das áreas. Com isso, somente um usuário com permissão de acesso poderá reabrir um período já encerrado no sistema para inclusão de novos lançamentos.

Esta validação de não permitir a realização de lançamentos para uma data encerrada é relevante, tendo em vista que a inclusão de lançamentos retroativos altera os saldos das contas contábeis e por consequência os valores gerados nos documentos enviados ao BACEN. Com isso, no caso de reabertura de período para lançamento retroativo, a instituição terá que reenviar os documentos ao BACEN.

4.2.5 APURAÇÃO DE RESULTADOS

Durante a realização da análise, identificou-se que as Instituições Financeiras estão obrigadas a realizar a Apuração de Resultados do Exercício duas vezes ao ano, nos meses de junho e dezembro. No Sistema de Contabilidade, a Apuração de Resultados é uma funcionalidade comandada pelo usuário, onde o sistema zera as contas de resultado credoras e devedoras automaticamente e transfere o saldo resultante para uma conta do Patrimônio Líquido informada pelo usuário.

O sistema conta com regras para não permitir que o usuário faça a Apuração de Resultados para o mesmo período mais de uma vez e possibilita que o usuário reverta a Apuração de Resultados, caso tenha feito incorretamente e realize o processo

ISSN – 2526-9526

novamente. Constatou-se que devido à relevância deste processo, as instituições concedem acesso a esta funcionalidade somente para os gerentes das áreas.

4.2.6 DOCUMENTOS BACEN

Para possibilitar o acompanhamento e supervisão do Sistema Financeiro Nacional (SFN), o BACEN exige das Instituições Financeiras o envio de uma série documentos, como por exemplo, o Balancete Patrimonial Analítico (mensal), conhecido como CADOC 4010 e o Balanço Patrimonial Analítico (semestral), conhecido como CADOC 4016.

Diante desta necessidade, constatou-se que o Sistema de Contabilidade possui uma funcionalidade específica para geração dessas informações, onde os documentos são gerados no *layout* estabelecido pelo BACEN, não sendo necessário que o usuário realize configurações manuais.

A geração e o envio dos documentos são realizados pelo usuário. No momento da geração, o sistema exibe em tela as informações e permite que seja impresso ou salvo o relatório para conferência. Para o envio das informações, é gerado um arquivo posicional no *layout* determinado pelo BACEN.

O sistema possui validações para identificar se o documento já foi gerado anteriormente e não permite que o usuário altere os valores gerados no documento, os quais retornam diretamente dos saldos das contas contábeis. As informações geradas nestes documentos são essenciais, pois expressam a situação econômico-financeira da Instituição Financeira. Por este motivo, as instituições concedem acesso a esta funcionalidade somente para os usuários responsáveis pela geração e envio dos Documentos.

4.2.7 GERAÇÃO E CONFIGURAÇÃO DE RELATÓRIOS

O Sistema de Contabilidade possui diversos relatórios padrões, tais como Balancetes de Saldos, Balanços, Razão Contábil, Demonstrações Contábeis, Balancete por Centro de Custos, entre outros. Além desses relatórios, o sistema possui uma funcionalidade chamada Relatórios Configurados, a qual possibilita que o usuário crie e parametrize relatórios e demonstrativos contábeis gerenciais de acordo com a sua necessidade, inclusive para atender demandas legais do BACEN.

Em todos os relatórios gerados pelo sistema ficam registradas informações como data e hora da geração, versão do sistema e do banco de dados, bem como o usuário que gerou o relatório. Verificou-se ainda, que os usuários acessam apenas os relatórios que estão associados ao seu perfil de acesso no Sistema de Segurança.

4.3 PERCEPÇÕES SOBRE EFETIVIDADE DOS CONTROLES PRESENTES NO SISTEMA DE CONTABILIDADE E SEGURANÇA DA INFORMAÇÃO

Esta seção apresenta as percepções dos usuários, analistas e desenvolvedores sobre a efetividade dos controles presentes no Sistema de Contabilidade.

4.3.1 PERCEPÇÕES DOS ANALISTAS E DESENVOLVEDORES

Nas entrevistas realizadas com os analistas e desenvolvedores examinou-se as percepções sobre a efetividade dos controles existentes no Sistema de Contabilidade, a relevância da segurança da informação para as instituições, os controles que

ISSN – 2526-9526

implementam em suas atividades e como percebem a importância que o usuário atribui a estes controles.

Inicialmente, foi questionado sobre a existência de relatórios de usuários, controles de acesso e auditoria. Os respondentes citaram que o sistema possui relatórios de usuários, relatórios de *logs* de acesso e permite a configuração de trilhas de auditoria por perfil e transação.

Porém, quando questionados se as funcionalidades existentes possibilitam controlar, autorizar e auditar todo e qualquer acesso às transações realizadas no Sistema de Contabilidade, ressaltaram que controlar e autorizar sim, mas auditar não, conforme pode ser visto no trecho do entrevistado 3 a seguir: "O sistema no qual trabalho prestando suporte aos clientes, possui relatórios de acesso aos usuários e relatórios de trilha de auditoria. Porém, a trilha é bastante limitada, não abrangendo todas as funcionalidades do sistema. Com relação ao relatório de usuários, o mesmo não demonstra a data de criação do usuário, apenas a data de última alteração de senha do mesmo".

Com isso, verificou-se que a funcionalidade de auditoria existente é limitada e necessita de melhorias para auditar e guardar todo o histórico das transações realizadas pelos usuários no Sistema de Contabilidade, assim como o relatório de usuários que poderia contemplar mais informações.

Quanto ao bloqueio de usuários após um número de tentativas consecutivas incorretas, os entrevistados destacaram que se configurado corretamente o sistema bloqueia o acesso do usuário, deixando-o com *status* suspenso. Neste caso, para que o usuário acesse o Sistema de Contabilidade, o administrador deve realizar a liberação do acesso do usuário novamente no Sistema de Segurança, sendo necessário o cadastramento de uma nova senha.

Acerca do registro de mudanças realizadas nas tabelas de controle de acesso e nas tabelas de manutenção de perfis e usuários, os desenvolvedores destacaram que em nível de tabelas todas podem ser auditadas, no entanto somente a última alteração fica registrada, como pode-se observar no trecho do entrevistado 5: "A auditoria normalmente se resume a última alteração feita".

Outro aspecto abordado foi sobre a proteção das tabelas de controle de acesso contra modificações ou acesso por usuários sem autorização. Os analistas responderam que as tabelas do banco de dados não estão protegidas. Os desenvolvedores complementaram destacando que as tabelas não possuem nenhum tratamento específico e que os controles existem somente em nível de tela do sistema, conforme pode ser verificado no trecho do entrevistado 5 a seguir: "As tabelas do banco de dados, não! Mas a tela do sistema por onde é feita a manutenção, sim! Só quem possui permissão a tela consegue fazer modificações de controle de acesso".

Nesta perspectiva, foi questionado se o Sistema de Segurança registra a data e hora do último acesso ao Sistema de Contabilidade. Os analistas relataram que o sistema grava todos os *logins* se estiver parametrizado. Os desenvolvedores esclareceram que o sistema registra a data e hora do último acesso do usuário, mas não de forma específica por sistema, uma vez que o acesso pode ter sido feito em algum outro sistema também controlado pelo Sistema de Segurança.

Quanto a associação de usuários a perfis de acesso, os analistas e desenvolvedores explicaram que o usuário possui apenas um perfil global, vinculado às

ISSN – 2526-9526

transações do sistema, ou seja, a associação entre usuário e perfil é única, enquanto que na associação entre perfil e sistema, pode-se associar um perfil para diversos sistemas. Dentro de um perfil, é possível associar vários usuários, onde todos terão acesso às mesmas funcionalidades.

Referente ao processo de acesso ao Sistema de Contabilidade, tanto os analistas quanto os desenvolvedores responderam que os usuários autorizados a acessar o sistema são identificados individualmente pelo Sistema de Segurança. Em relação à possibilidade de restringir o acesso de um usuário por funções (botões) da tela, conforme consta no manual do sistema, todos responderam que é possível fazer este tipo de configuração.

Sobre a parametrização de políticas de senhas, tanto os analistas quanto os desenvolvedores, relataram que o sistema possui uma funcionalidade que permite algumas configurações, tais como, tamanho mínimo, quantidade de letras e números e não permitir reutilização de senha.

Por fim, verificou-se as percepções sobre a importância da segurança da informação e sobre os controles que cada um utiliza no desenvolvimento das suas atividades. De modo geral, todos responderam ser fundamental a implementação de políticas de segurança da informação, conforme pode ser visto no trecho do entrevistado 1: "Considero ser importantíssima a implementação de segurança adequada e completa em sistemas corporativos. Acredito ser importante ter uma equipe de segurança 'olhando' para esta questão, ou seja, uma forte equipe de Governança que auxilia na definição da política, na implementação da política de segurança e também na auditoria nos sistemas".

Tanto os analistas quanto os desenvolvedores destacaram que os controles de permissão de acesso as funcionalidades do sistema são extremamente relevantes para garantir a integridade dos dados gerados no Sistema de Contabilidade. Salientaram ainda, que a implementação de controles do tipo, *firewall*, criptografia, sistemas biométricos, antivírus, e principalmente a ética podem auxiliar no processo de segurança da informação.

Os desenvolvedores mencionaram que todos os controles utilizados pelos sistemas já foram desenvolvidos no Sistema de Segurança, sendo necessário apenas conceder as permissões de acesso nas novas funcionalidades, como pode-se verificar no trecho do entrevistado 4: "Acho extremamente importante o controle de permissão/acesso. Todos os nossos controles já foram desenvolvidos no Sistema de Segurança. Precisamos apenas dar as permissões nas novas funcionalidades". Além disso, citaram que normalmente não se envolvem diretamente com as rotinas de segurança, pois elas são implementadas no *framework* do sistema, de forma genérica para todas as rotinas.

A respeito da percepção sobre a importância que o usuário do sistema atribui aos controles existentes e sobre a segurança da informação, verificou-se opiniões diversas. Alguns analistas e desenvolvedores destacaram que a percepção é que o usuário final não dá muita importância, de maneira que só percebe a existência destes mecanismos quando não possui acesso a uma tela ou relatório.

Outros percebem que o usuário só reconhece a importância da segurança da informação quando é afetado negativamente, como pode ser visto no trecho do entrevistado 1: "Percebo que o usuário só dá a real importância quando é afetado

ISSN – 2526-9526

negativamente de alguma forma. Se nunca teve problemas, se nunca "sofreu", se nunca foi prejudicado, dificilmente o usuário será a favor da implementação de uma política forte e bem definida. O usuário deseja ter acesso ao sistema e muitas vezes, as questões de segurança, não são bem aceitas, são vistas como um "entrave" às suas atividades diárias".

Os analistas destacaram ainda que com exceção dos profissionais da área contábil e do setor de segurança da informação, os demais usuários não se importam tanto e até desconhecem as regras de segurança para acesso e manutenção de informações do sistema, conforme exposto no trecho do entrevistado 3: "Com exceção dos profissionais de contabilidade, controladoria e do setor de segurança da informação, percebo que os demais usuários em sua maioria desconhecem regras de segurança para acesso e manutenção de informações do sistema".

4.3.2 PERCEPÇÕES DOS USUÁRIOS

Nas entrevistas realizadas com os usuários do Sistema de Contabilidade, buscou-se verificar as percepções sobre segurança da informação e sobre os controles de acesso presentes no sistema. Os usuários entrevistados são membros de três Instituições Financeiras de relevância no mercado.

Os usuários relataram que as instituições onde trabalham possuem políticas de segurança da informação, as quais são apresentadas para todos os funcionários. Mencionaram também, que na integração de um novo funcionário é assinado um termo de ciência sobre estas políticas.

Além disso, destacaram que as instituições adotam controles de acesso a *sites*, políticas de senhas, plano de contingência, *backup*, documentos que envolvem sigilo bancário, revisão de perfis de acesso aos sistemas e gestão de mudanças de sistemas para evitar incidentes envolvendo a segurança da informação.

Verificou-se que as instituições possuem uma equipe para administração, monitoramento e revisão das políticas de segurança da informação, como pode ser visto no trecho do entrevistado 8 a seguir: "Sim, a norma é revisada no mínimo uma vez por ano e apresentada para a gestão da empresa".

Identificou-se também, que as instituições estão investindo em treinamentos para aprimorar as políticas de segurança da informação, como pode ser constatado no trecho do entrevistado 9: "Os integrantes da equipe recebem treinamento e fazem visitas em outras grandes empresas para troca de conhecimentos". Este aspecto reforça os resultados obtidos por Klein (2014), onde foi constatado que a realização de treinamentos e orientações sobre segurança da informação, são fundamentais para aprimorar a percepção dos usuários acerca da severidade das ameaças, a gravidade dos danos que podem ser causados, bem como os benefícios gerados ao serem adotados controles adequados.

Por meio das entrevistas também foi possível examinar que como as Instituições Financeiras trabalham com informações confidenciais dos seus clientes, existe uma grande preocupação com questões de sigilo bancário, como pode ser observado no trecho do entrevistado 10 a seguir: "Em função da sensibilidade das informações que a empresa processa, há uma grande preocupação com questões de sigilo bancário".

Diante destas preocupações com a segurança da informação, pode-se afirmar que semelhante aos resultados obtidos nos estudos de Silva (2013), os usuários

ISSN – 2526-9526

entrevistados estão conscientes da importância dos controles e das políticas de segurança para promover maior segurança da informação e confiabilidade das informações geradas nos sistemas de informação.

Outro ponto levantado nas entrevistas, foi sobre a confidencialidade das senhas. Os usuários destacaram que estão cientes que as senhas de acesso aos sistemas são de uso pessoal e intransferível e que é responsabilidade de cada um manter o sigilo. Além disso, o compartilhamento de senhas é punido por severas regras, como pode ser visto no trecho do entrevistado 9 a seguir: "A senha é individual e intransferível. É responsabilidade de cada um manter o sigilo. O compartilhamento da senha é punido com severas regras. Dentre elas até com o desligamento da empresa".

Na sequência, direcionou-se a entrevista para questões envolvendo os controles de acesso ao Sistema de Contabilidade. Verificou-se que os usuários conhecem o Sistema de Segurança e a forma como são definidos os acessos, visto que relataram que as permissões de acesso são realizadas através de perfis de acesso, como pode ser visto no trecho do entrevistado 10 a seguir: "O acesso ao sistema da contabilidade é liberado através de perfis. Desta forma, o acesso é liberado somente para as funções restritas de cada funcionário" e no trecho do entrevistado 8: "O acesso na contabilidade é restrito aos funcionários da área de controladoria. Está dividido em dois perfis: analista contábil e contábil super".

Quando questionados sobre a ocorrência de violação de acesso ao Sistema de Contabilidade, os usuários mencionaram que até o momento não tiveram nenhum incidente de acesso não autorizado, como pode ser visto no trecho do entrevistado 8 a seguir: "Não temos casos de acessos não autorizados. Desta forma o sistema não é violado".

Quanto à existência de distorções ou erros nas informações geradas no Sistema de Contabilidade, os usuários relataram que eventualmente podem ser encontradas inconsistências nas informações originadas do Sistema de Créditos, conforme pode ser verificado no trecho do entrevistado 9 a seguir: "Eventualmente sim, algumas inconsistências podem ser encontradas nas informações Crédito X Contabilidade".

Questionou-se ainda, sobre a satisfação com os controles de acesso existentes no Sistema de Contabilidade. As respostas foram positivas, como pode ser verificado no trecho do entrevistado 10 a seguir: "Estou satisfeito com os controles de acessos existentes. Temos uma equipe de Riscos e Compliance responsável nos controles de acessos. A revisão dos acessos é realizada semestralmente".

Por fim, os usuários sugeriram que além dos relatórios de *logs* e acessos, fosse criado um novo relatório no Sistema de Segurança para extração da lista de todos os usuários cadastrados no sistema e a sua situação (em atividade, bloqueado, suspenso), conforme pode ser verificado no trecho do entrevistado 8 a seguir: "Gostaria que o sistema tivesse um relatório para extração de todos os usuários cadastrados, pois esta é uma informação que costuma ser solicitada pela auditoria externa e atualmente a listagem é extraída diretamente do banco de dados".

Diante do exposto, pode-se afirmar que os resultados alcançados neste estudo reforçam os aspectos abordados nos estudos relacionados, uma vez que constatou-se a importância da realização de treinamentos sobre segurança da informação, examinou-se que a satisfação do usuário com as práticas de segurança é essencial para o sucesso de um sistema e verificou-se que as percepções dos analistas, desenvolvedores e

ISSN – 2526-9526

usuários sobre a efetividade dos controles presentes nos sistemas de informação são relevantes para as instituições, tendo em vista os problemas enfrentados atualmente, envolvendo a segurança da informação.

5 CONSIDERAÇÕES FINAIS

O objetivo deste estudo foi identificar as percepções dos analistas, desenvolvedores e usuários acerca da efetividade dos controles de acesso presentes em um Sistema de Contabilidade para Instituições Financeiras, tendo como base os atributos da segurança da informação.

Constatou-se que os controles de acesso são realizados por um Sistema de Segurança, o qual permite uma série de configurações a partir da criação de perfis de acesso, onde é possível autorizar o acesso em nível de menus, telas e até funções (botões) ao Sistema de Contabilidade. Além disso, verificou-se que o Sistema de Contabilidade possui diversas regras e validações em suas funcionalidades que contribuem para a integridade das informações geradas no sistema. No entanto, cabe salientar, que foram identificadas possibilidades de melhorias no Sistema de Segurança, como por exemplo, na funcionalidade de trilha de auditoria para passar a auditar todas as transações do Sistema de Contabilidade e criação de um novo relatório que possibilite a extração da listagem de usuários de forma mais simples e ágil.

Os dados obtidos a partir da realização das entrevistas demonstraram que tanto na percepção dos usuários quanto para os analistas e desenvolvedores, os controles de acesso presentes no Sistema de Contabilidade são efetivos, pois garantem que somente usuários autorizados acessem as funcionalidades e relatórios do sistema. Quanto ao valor da segurança da informação nas instituições, verificou-se que as Instituições Financeiras onde os usuários trabalham adotam políticas de segurança, estão preocupadas com estas questões e reconhecem o poder das informações geradas nos sistemas de informação. No entanto, nas percepções dos analistas e desenvolvedores do sistema, a maioria dos usuários preocupa-se com estas questões somente quando ocorre algum tipo de incidente envolvendo segurança da informação.

Diante do estudo apresentado, comprovou-se a essencialidade de serem adotados controles de acesso efetivos nos sistemas de informação e a relevância da capacitação dos usuários dos sistemas para que compreendam a importância da segurança da informação e adotem os controles durante a realização das suas atividades. No que refere à contribuição deste estudo para a vida acadêmica, pode-se afirmar que houve um acréscimo de conhecimento considerável a respeito do tema, uma vez que foi possível verificar na prática como os aspectos sobre segurança da informação vistos em aula são aplicados no dia a dia das instituições. Além disso, constatou-se o quanto o usuário (componente humano) é importante para garantir maior segurança nos sistemas de informação, pois atualmente os sistemas já são desenvolvidos com rotinas para atender os requisitos da segurança da informação.

Importante ressaltar, ainda, que o intuito desta pesquisa não foi esgotar a discussão a respeito do tema, mas sim explorar o contexto atual da segurança da informação em sistemas de informações contábeis, tendo em vista a relevância das informações geradas na Contabilidade para tomada de decisão nas instituições. Com isso, existem possibilidades de aprofundar o tema para realizar estudos que contribuam

ISSN – 2526-9526

para o entendimento das percepções dos usuários de sistemas de informação para formulação de políticas de segurança mais efetivas e eficazes nas organizações.

REFERÊNCIAS

ARAÚJO, Adriana M. Procópio de; ASSAF NETO, Alexandre. **Aprendendo contabilidade**.
São Paulo: Inside Books, 2010.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:** Tecnologia da informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:** Tecnologia da informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013.

BALTZAN, Paige; PHILLIPS, Amy. **Sistemas de informação**. Porto Alegre: AMGH, 2012.

BEAL, Adriana. **Segurança da informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. Porto Alegre: Atlas, 2007. Disponível em: < https://integrada.minhabiblioteca.com.br/#/books/9788522472109/>. Acesso em: 13 jun. 2018.

FONTES, Edison. **Segurança da informação**. São Paulo: Saraiva, 2010. Disponível em: < https://integrada.minhabiblioteca.com.br/#/books/9788502122185/>. Acesso em: 13 jun. 2018.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo (Org.). **Métodos de pesquisa**. Porto Alegre: EDUFRGS, 2009. 120p. Disponível em:<www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf.>. Acesso em: 13 jun. 2018.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social.**5. ed. São Paulo: Atlas, 1999.

HURT, Robert L. **Sistemas de informações contábeis**: conceitos básicos e temas atuais. 3. ed. Porto Alegre: AMGH, 2014.

IMONIANA, Joshua Onome. **Auditoria de sistemas de informação**. 2. ed. São Paulo: Atlas, 2011.

KLEIN, Rodrigo Hickmann. **Ameaças, controle, esforço e descontentamento do usuário no comportamento seguro em relação à Segurança da Informação.**

ISSN – 2526-9526

Disponível em: < http://tede2.pucrs.br/tede2/bitstream/tede/5671/1/456919.pdf >. Acesso em: 13 jun. 2018.

PADOVEZE, Clóvis Luís. **Sistemas de informações contábeis:** fundamentos e análises. 6. ed. São Paulo: Atlas, 2009.

RAINER JR, R. Kelly; CEGIELSKI, Casey G. **Introdução a sistemas de informação:** apoiando e transformando negócios na era da mobilidade. 3. ed. Rio de Janeiro: Elsevier, 2011.

SILVA, Wagner Lima da. **Segurança da informação:** um estudo sobre a percepção do usuário da informação contábil. Disponível em: < http://tede.mackenzie.br/jspui/bitstream/tede/891/1/Wagner%20Lima%20da%20Silva.pdf >. Acesso em: 13 jun. 2018.

YIN, Robert K. **Estudo de caso:** planejamento e métodos. 3. ed. Porto Alegre: Bookman, 2005.